

# ESTIMATING THE NUMBER OF ROOTS OF TRINOMIALS OVER FINITE FIELDS

ZANDER KELLEY\*, SEAN W. OWEN\*

**ABSTRACT.** We show that univariate trinomials  $x^n + ax^s + b \in \mathbb{F}_q[x]$  can have at most  $\delta \left\lfloor \frac{1}{2} + \sqrt{\frac{q-1}{\delta}} \right\rfloor$  distinct roots in  $\mathbb{F}_q$ , where  $\delta = \gcd(n, s, q-1)$ . We also derive explicit trinomials having  $\sqrt{q}$  roots in  $\mathbb{F}_q$  when  $q$  is square and  $\delta = 1$ , thus showing that our bound is tight for an infinite family of finite fields and trinomials. Furthermore, we present the results of a large-scale computation which suggest that an  $O(\delta \log q)$  upper bound may be possible for the special case where  $q$  is prime. Finally, we give a conjecture (along with some accompanying computational and theoretical support) that, if true, would imply such a bound.

## 1. INTRODUCTION

For univariate polynomial equations defined over a field, it is desirable to obtain general upper bounds on the number of solutions given in simple terms of plainly available information, such as the coefficients, exponents, or number of terms. The ubiquitous example of this is the degree bound, but over non-algebraically closed fields, it is possible to considerably improve upon the degree bound for certain non-negligible families of polynomials. Over the real numbers, Descartes' Rule of Signs implies that a  $t$ -nomial  $f$  must have less than  $2t$  real roots. For sparse polynomials - those with a small number of nonzero terms - this can provide a remarkable improvement on the trivial upper estimate given by the degree of  $f$ .

In [5], the authors establish a finite field analogue of Descartes' Rule: a sparsity-dependent upper bound on the number of roots of a  $t$ -nomial over  $\mathbb{F}_q$ . More recently, an improved upper bound was derived in [9]. Here, we investigate possible further improvements to the bound for the special case of  $t = 3$ . This can be considered the smallest nontrivial choice of  $t$ , since the zero sets of univariate binomials are easily characterized - they are simply cosets of subgroups of  $\mathbb{F}_q^*$ , possibly together with  $0 \in \mathbb{F}_q$ .

**Theorem 1.1.** [9, Theorems 2.2 and 2.3] *Let*

$$f(x) = c_1x^{a_1} + c_2x^{a_2} + \cdots + c_tx^{a_t} \in \mathbb{F}_q[x]$$

*with all  $c_i$  nonzero and  $a_1 > a_2 > \cdots > a_t = 0$ . If  $f$  vanishes on an entire coset of a subgroup  $H \subseteq \mathbb{F}_q^*$ , then*

$$\#H \in \{k \in \mathbb{N} : \text{for each } a_i, \text{ there is an } a_j \text{ with } j \neq i \text{ and } a_i \equiv a_j \pmod{k}\}.$$

*Furthermore, let  $R(f)$  denote the number of distinct roots of  $f$  in  $\mathbb{F}_q$ , and suppose  $R(f) > 0$ . If  $C$  denotes the maximal cardinality of a coset on which  $f$  vanishes, then*

$$R(f) \leq 2(q-1)^{1-1/(t-1)}C^{1/(t-1)}.$$

---

\*Partially supported by NSF grants DMS-1156589, DMS-1460766, and CCF-140902.

For a trinomial  $f(x) = x^n + ax^s + b \in \mathbb{F}_q[x]$ , with  $a$  and  $b$  nonzero, associate the parameter

$$\delta = \gcd(n, s, q - 1).$$

Suppose that  $R(f) > 0$ . It follows from Theorem 1.1 that if  $f$  vanishes on a coset of size  $C$ , then  $n \equiv s \equiv 0 \pmod{C}$ . Since  $C$  must divide  $\#\mathbb{F}_q^*$ , we have that  $C$  divides  $\delta$ . On the other hand, if  $f$  vanishes at  $\alpha \in \mathbb{F}_q$ , then  $\alpha \in \mathbb{F}_q^*$ , and  $f$  vanishes on the entire coset  $\{x \in \mathbb{F}_q^* : x^\delta = \alpha^\delta\}$  of order  $\delta$ . So, in the trinomial case we have explicitly that  $C = \delta$ , and the bound given above simplifies to

$$R(f) \leq 2\sqrt{\delta(q-1)}.$$

As pointed out in [6], this bound for trinomials is also a consequence of an earlier result from [3] which bounds the number of cosets  $S_i \subset \mathbb{F}_q^*$  needed to express the zero set of a sparse polynomial as a union of the form  $\bigcup_{i=1}^N S_i$ . Our first result refines this upper bound.

**Theorem 1.2.** *The roots of a trinomial*

$$f(x) = x^n + ax^s + b \in \mathbb{F}_q[x]$$

are the union of no more than  $\left\lfloor \frac{1}{2} + \sqrt{\frac{q-1}{\delta}} \right\rfloor$  cosets of the subgroup  $H \subseteq \mathbb{F}_q^*$  of size  $\delta$ .

Consequently, we now have  $R(f) \leq \delta \left\lfloor \frac{1}{2} + \sqrt{\frac{q-1}{\delta}} \right\rfloor$ , improving the previous result by approximately a factor of 2 when  $\delta \ll q$ . The method of proof is elementary but interesting: given a trinomial with  $\delta = 1$  and  $r$  roots in a field of undetermined size, we construct  $r^2 - r + 1$  distinct nonzero elements in the field, giving a lower bound on its size.

Additionally, we show that when  $\delta = 1$ , this new bound is optimal for even-degree extensions of  $\mathbb{F}_p$ . If  $q$  is an even power of a prime  $p$  and  $\delta = 1$ , the bound reduces to  $R(f) \leq \sqrt{q}$ , and we can indeed construct trinomials with  $\delta = 1$  and  $\sqrt{q}$  distinct roots in  $\mathbb{F}_q$ .

**Theorem 1.3.** *For any odd prime  $p$ , the trinomial  $x^{p^k} + x - 2$  has exactly  $p^k$  roots in  $\mathbb{F}_{p^{2k}}$ .*

We prove Theorem 1.3 via linear-algebraic techniques: the extremal examples provided are translations of linear maps with null-spaces of exactly half the dimension of  $\mathbb{F}_q$  as a vector space over  $\mathbb{F}_{\sqrt{q}}$ . The optimality of the bound is somewhat murkier when  $\mathbb{F}_q$  is not an even-degree extension. Trinomials with nearly as many roots have been found for some other cases; for example, when  $q$  is a cube, the authors of [6] give the example  $f(x) = x^{1+q^{1/3}} + x + 1$  which has  $q^{1/3} + 1$  roots.

Most notably, the question of optimality of the bound remains open for the prime field case. We remark that out of all examples of which we are aware, including those given in [6], the only sparse polynomials which vanish at a substantial number of points do so by abusing some obvious algebraic structure of  $\mathbb{F}_q$  - they either vanish on an entire translation of a subspace or on an entire coset of a nontrivial subgroup. Trinomials over prime fields which have  $\delta = 1$  are deprived of both of these luxuries, and accordingly, finding examples with many roots seems to be difficult.

Let  $R_p$  denote the maximum value of  $R(f)$  over all trinomials in  $\mathbb{F}_p[x]$  having  $\delta = 1$ . Recall that by Fermat's little theorem, if  $\tilde{n} \equiv n \pmod{p-1}$  and  $\tilde{s} \equiv s \pmod{p-1}$ , then the two polynomials  $f(x) = x^n + ax^s + b$  and  $\tilde{f}(x) = x^{\tilde{n}} + ax^{\tilde{s}} + b$  define the same mapping on  $\mathbb{F}_p^*$ , so it is possible to compute  $R_p$  in straightforward way by enumerating trinomials with degree less than  $p-1$  and counting their roots. In [6],  $R_p$  is computed for all primes up to 16633, and they find no instances in which  $R_p$  exceeds  $2 \log p$ . As a result of a large-scale computation, we observe that the inequality  $R_p \leq 2 \log p$  continues to hold for all primes up to 139571. Therefore, it appears that the current bound,  $R_p = O(\sqrt{p})$ , is still far

from optimal for trinomials over  $\mathbb{F}_p$ , but we have been unsuccessful in proving any stronger version of Theorem 1.2 for prime fields.

It is known that if  $f$  is allowed to range over all polynomials in  $\mathbb{F}_p[x]$ , the distribution of  $R(f)$  approaches a Poisson distribution with mean 1 as  $p \rightarrow \infty$  [12]. That is, the proportion of  $f \in \mathbb{F}_p[x]$  with  $R(f) = r$  is approximately  $e^{-1}/r!$  when  $p$  is sufficiently large. Based on computational experiments, this also appears to be true when  $f$  ranges over just the set of trinomials in  $\mathbb{F}_p[x]$  with  $\delta = 1$ . This is certainly *not* the case if  $f$  were to range over, for example, the set of *all* trinomials, or the set of *tetranomials* with  $\delta = 1$  due to the presence of  $f$  which vanish on large cosets. On the other hand, the set of trinomials with  $\delta = 1$  appears to behave similarly to what we would expect from an  $f$  randomly selected from all of  $\mathbb{F}_p[x]$ . Apparently, restriction of  $f \in \mathbb{F}_p[x]$  to trinomial with  $\delta = 1$  provides very little statistical information about  $R(f)$ .

**Heuristic 1.4.** *With respect to root number, the set of trinomials  $f \in \mathbb{F}_p[x]$  with  $\delta = 1$  behaves like a uniform random sample of polynomials from  $\mathbb{F}_p[x]$ . That is, when  $p$  is large enough, the values of  $R(f)$  behave like they are given by random variables with distribution function  $\rho(r) = e^{-1}/r!$  (a Poisson distribution with mean 1).*

In Section 4, we show that Heuristic 1.4 allows us to make fairly accurate guesses of the actual values of  $R_p$  recorded by our computations. Therefore, it may be that the observed logarithmic growth of  $R_p$  is not due to any special property of trinomials with  $\delta = 1$ , but rather emerges as a statistical consequence of this set being so “ordinary,” together with the exponential decay of the Poisson distribution. We phrase this formally as the following conjecture that the distributions of  $R(F)$  and  $R(f)$ , with  $F$  ranging over  $\mathbb{F}_p[x]$  and  $f$  ranging over trinomials with  $\delta = 1$ , differ by at most a constant factor.

**Conjecture 1.5.** *Define*

$$M_p = \{f \in \mathbb{F}_p[x] : \deg f < p\},$$

$$T_p = \{x^n + ax^s + b : (a, b) \in (\mathbb{F}_p^*)^2, 0 < s < n < p - 1, \text{ and } \gcd(n, s, p - 1) = 1\}.$$

Let  $\mu(p, r)$  denote the proportion of  $f \in M_p$  with  $R(f) = r$  and  $t(p, r)$  denote the proportion of  $f \in T_p$  with  $R(f) = r$ . There exists a constant  $\lambda \in \mathbb{R}$  such that

$$t(p, r) \leq \lambda \mu(p, r),$$

for all  $p$  prime and  $r \in \mathbb{N}$ .

If these two distributions do in fact differ by at most a constant factor, then we are able to readily derive the logarithmic upper bound for  $R_p$  suggested by our experiments. And, in turn, we could extend such a bound to trinomials with  $\delta > 1$  by noticing that  $x^n + ax^s + b$  has at most  $\delta$  roots for every root of  $x^{n/\delta} + ax^{s/\delta} + b$ .

**Corollary 1.6.** *Suppose Conjecture 1.5 is true. Then, we have the asymptotic bound*

$$R_p = \max\{R(f) : f \in T_p\} = O\left(\frac{\log p}{\log \log p}\right).$$

*Proof.* Let  $M_p(r) = \{f \in M_p : R(f) = r\}$  and  $T_p(r) = \{f \in T_p : R(f) = r\}$  so that

$$\mu(p, r) = \frac{\#M_p(r)}{\#M_p} \text{ and } t(p, r) = \frac{\#T_p(r)}{\#T_p}.$$

We can bound  $\#M_p(r)$  from above by counting polynomials of the form

$$\left( \prod_{i=1}^r (x - \alpha_i) \right) \left( \sum_{i=0}^{p-1-r} c_i x^i \right),$$

with  $\alpha_i \in \mathbb{F}_p$  distinct, which gives

$$\mu(p, r) = \frac{\#M_p(r)}{\#M_p} = \frac{\#M_p(r)}{p^p} \leq \frac{\binom{p}{r} p^{p-r}}{p^p} = \binom{p}{r} \frac{1}{p^r} \leq \frac{1}{r!}.$$

Obviously  $\#T_p \leq p^4$ , so assuming the existence of  $\lambda$  defined in Conjecture 1.5, we have

$$\#T_p(r) \leq \lambda \mu(r, p) \#T_p \leq \frac{\lambda \#T_p}{r!} \leq \frac{\lambda p^4}{r!}.$$

If  $\lambda p^4/r! < 1$  then the set  $T_p(r)$  is empty, so we must have  $\lambda p^4/R_p! \geq 1$ , or equivalently,  $\log(R_p!) \leq \log(\lambda p^4)$ . By applying Stirling's approximation, we get the asymptotic bound

$$R_p \log R_p \sim \log(R_p!) \leq \log(\lambda p^4) = 4 \log p + \log \lambda = O(\log p).$$

By considering the growth order of the inverse function of  $y = x \log x$ , we obtain

$$R_p = O\left(\frac{\log p}{\log \log p}\right).$$

□

We remark that in [6], it is shown that under the Generalized Riemann Hypothesis, there exists an infinite sequence of primes  $(p_k)_{k=1}^\infty$  satisfying the lower bound  $R_{p_k} = \Omega\left(\frac{\log p_k}{\log \log p_k}\right)$ . So, the truth of both Conjecture 1.5 and GRH would imply that the bound in Corollary 1.6 is, up to a multiplicative constant, asymptotically optimal.

Finally, we prove the following theoretical result which states that Conjecture 1.5 is true if we consider only trinomials of bounded degree as we take  $p$  to infinity. This weaker result is suggestive but certainly not sufficient to imply the bound in Corollary 1.6. In particular, Theorem 1.7 shows the existence of  $\lambda_N \in \mathbb{R}$  such that  $t_N(p, r) \leq \lambda_N \mu(p, r)$ , but we do not have a bound on the set  $\{\lambda_N : N \in \mathbb{N}\}$ .

**Theorem 1.7.** *Suppose  $n, s \in \mathbb{N}$  with  $0 < s < n$  and  $\gcd(n, s) = 1$ . As  $p \rightarrow \infty$ , the proportion of pairs  $(a, b) \in (\mathbb{F}_p^*)^2$ , such that  $f(x) = x^n + ax^s + b$  has  $R(f) = r$ , converges to*

$$\begin{cases} \frac{[e^{-1}(n-r)!]}{r!(n-r)!} & \text{if } r < n \\ 1/r! & \text{if } r = n, \end{cases}$$

where  $[\cdot]$  denotes the “nearest integer” function.

Furthermore, fix  $N \in \mathbb{N}$ , and let

$$T_{p,N} = \{x^n + ax^s + b : (a, b) \in (\mathbb{F}_p^*)^2, 0 < s < n \leq N, \text{ and } \gcd(n, s, p-1) = 1\}.$$

Let  $\mu(p, r)$  be defined as in Conjecture 1.5, and let  $t_N(p, r)$  denote the proportion of  $f \in T_{p,N}$  with  $R(f) = r$ . We then have

$$\limsup_{p \rightarrow \infty} \left( \max_{r \leq N} \frac{t_N(p, r)}{\mu(p, r)} \right) \leq e.$$

## 2. NEW UPPER BOUND AND EXTREMAL TRINOMIALS

**Definition 2.1.** For  $n, s$  fixed, define the family of trinomials in  $\mathbb{F}_q[x]$

$$C(n, s) = \{f_c(x) = cx^n - (c+1)x^s + 1 : c \neq -1, 0\}.$$

Observe that  $C(n, s)$  is exactly the set of trinomials with

- support  $\{n, s, 0\}$
- constant term 1
- $f(1) = 0$

This is clear because  $f(1) = 0$  if and only if  $f$ 's coefficients sum to zero. We introduce this family of trinomials because they have the following useful property.

**Lemma 2.2.** *Let  $G \subseteq \mathbb{F}_q^*$  be the unique multiplicative subgroup of order  $N$ , and suppose that  $\gcd(n, s, N) = 1$ . The only root in  $G$  shared by any two members of  $C(n, s)$  is  $\alpha = 1$ .*

*Proof.*  $f_c(\alpha) = 0$  is equivalent to the following linear equation in  $c$ :

$$c(\alpha^n - \alpha^s) = \alpha^s - 1.$$

This has multiple solutions in  $c$  if and only if both  $\alpha^n - \alpha^s = 0$  and  $\alpha^s - 1 = 0$ . Since  $G$  is a cyclic group of order  $N$  and  $\gcd(n, s, N) = 1$ , the only  $\alpha \in G$  such that  $\alpha^n = \alpha^s = 1$  is  $\alpha = 1$  itself. So 1 is the only  $\alpha$  such that  $f_c(\alpha) = 0$  for multiple  $f_c \in C(n, s)$ .  $\square$

**Lemma 2.3.** *Let  $G \subseteq \mathbb{F}_q^*$  be the unique multiplicative subgroup of order  $N$ , and let  $f \in \mathbb{F}_q[x]$  be a trinomial of the form  $ax^n + bx^s + 1$  satisfying  $\gcd(n, s, N) = 1$ . The number of roots of  $f$  that lie in  $G$  does not exceed*

$$\frac{1}{2} + \sqrt{N}.$$

*Proof.* Suppose  $f(x) = ax^n + bx^s + 1$  has  $r$  distinct roots  $\zeta_1, \zeta_2, \dots, \zeta_r$  in  $G$ . For each  $\zeta_i$  let  $g_i(x) = f(\zeta_i x) = (a\zeta_i^n)x^n + (b\zeta_i^s)x^s + 1$ . Since the map  $x \rightarrow \zeta_i x$  permutes the elements of  $G$ , each of these  $g_i$  also has  $r$  roots in  $G$ . Additionally, each  $g_i$  is a member of  $C(n, s)$ , since  $g_i(1) = f(\zeta_i) = 0$ .

We now check that each  $g_i$  is distinct. Suppose  $g_i = g_j$  with  $i \neq j$ . We then have both  $\zeta_i^n = \zeta_j^n$  and  $\zeta_i^s = \zeta_j^s$ , or, equivalently,  $(\zeta_i/\zeta_j)^n = 1$  and  $(\zeta_i/\zeta_j)^s = 1$ . Once again, the only  $\alpha \in G$  that satisfies  $\alpha^n = \alpha^s = 1$  is  $\alpha = 1$ , so  $\zeta_i = \zeta_j$ , which contradicts the supposition that the roots  $\zeta_1, \zeta_2, \dots, \zeta_r$  are distinct.

In summary, there exist  $r$  distinct trinomials of  $C(n, s)$  that each have  $r$  roots in  $G$ , and by Lemma 2.2,  $\zeta = 1$  is the only root among these that is not unique. This implies that  $G$  contains at least  $r(r-1)+1$  distinct elements, but we know that  $G$  has size  $N$  by hypothesis. Therefore it must be that

$$r^2 - r + 1 \leq N,$$

which yields the desired constraint on  $r$ :

$$r \leq \frac{1}{2} + \sqrt{N}.$$

$\square$

We now have everything we need to complete the proof.

*Proof of Theorem 1.2.* Let  $f(x) = x^n + ax^s + b \in \mathbb{F}_q[x]$ . Obviously the roots of  $f$  are not affected by re-scaling; let

$$\tilde{f}(x) = \frac{1}{b}x^n + \frac{a}{b}x^s + 1 = \alpha x^n + \beta x^s + 1.$$

The exponents may fail to satisfy  $\delta = \gcd(n, s, q-1) = 1$ . However,  $\tilde{f}(x) = 0$  is equivalent to the system

$$\begin{aligned}\alpha y^{n/\delta} + \beta y^{s/\delta} + 1 &= 0 \\ y &= x^\delta.\end{aligned}$$

The second equation is only solvable for  $x$  when  $y$  lies in the subgroup of order  $(q-1)/\delta$ . The first equation satisfies  $\gcd(n/\delta, s/\delta, (q-1)/\delta) = 1$ , so we can invoke Lemma 2.3 and find that there are at most  $\left\lfloor \frac{1}{2} + \sqrt{\frac{q-1}{\delta}} \right\rfloor$  such  $y$ . Each of these  $y$  then admits one coset of  $\delta$  distinct solutions for  $x$ .  $\square$

*Proof of Theorem 1.3.* Observe that the function

$$T(x) = x^{p^k} + x$$

is an  $\mathbb{F}_{p^k}$ -linear map from  $\mathbb{F}_{p^{2k}}$  to  $\mathbb{F}_{p^{2k}}$ .  $T$  is a binomial, so it is easy to show that it does have nonzero solutions and therefore has a null space of positive dimension. Since  $T$  is not the zero transformation, we conclude that it has a null space of dimension 1, and therefore that it has  $p^k$  roots.

We see that  $f(x) = T(x) - 2 = 0$  exactly when  $T(x) = 2$ . This has one obvious solution,  $x = 1$ , so we conclude from the linearity of  $T$  that it has as many solutions as  $T(x) = 0$ . Therefore,  $f$  has  $p^k = \sqrt{q}$  roots, all of which are nonzero.  $\square$

### 3. PROOF OF THEOREM 1.7

Our proof of Theorem 1.7 relies on the following statement from [2], which can be viewed as a Chebotarev density theorem for function fields. At its core, this result is powered by the Lang-Weil estimate for the number of points on varieties over  $\mathbb{F}_q$ .

**Theorem 3.1.** [2, Proposition 3.1] *Let  $n, m$ , and  $N$  be positive integers, and let  $F \in \mathbb{F}_q[A_1, \dots, A_m, x]$  be separable in  $x$  and have  $\deg F \leq N$  and  $\deg_x F = n$ . Let  $\mathbb{F}$  be an algebraic closure of  $\mathbb{F}_q$ , and suppose that*

$$\text{Gal}(F, \mathbb{F}(A_1, \dots, A_m)) \cong S_n.$$

*For a partition  $\lambda$  of  $n$ , let  $C_\lambda \subset S_n$  denote the conjugacy class of permutations  $\sigma \in S_n$  with cycle type  $\lambda$ , and let  $\mathcal{A}_\lambda$  denote the set of  $(a_1, \dots, a_m) \in \mathbb{F}_q^m$  such that the univariate polynomial  $f(x) = F(a_1, \dots, a_m, x)$  factorizes over  $\mathbb{F}_q$  into irreducible factors with degree pattern  $\lambda$ . Then, there exists a constant  $c(m, N) \in \mathbb{R}$ , which depends only on  $m$  and  $N$ , such that*

$$\left| \frac{\#\mathcal{A}_\lambda}{q^m} - \frac{\#C_\lambda}{\#S_n} \right| \leq \frac{c(m, N)}{q^{1/2}}.$$

Let  $k$  be a field, and let  $F(x) = x^n + Ax^s + B$ , where  $A$  and  $B$  are indeterminates over  $k$ ,  $0 < s < n$ , and  $\gcd(n, s) = 1$ . It is shown by Cohen in [7, p. 64 and Corollary 3] that unless  $\text{char}(k)$  divides  $n(n-1)$ ,  $F$  is separable over  $k(A, B)$  and  $\text{Gal}(F, k(A, B)) \cong S_n$ . Here we consider  $k$  an algebraic closure of a prime field  $\mathbb{F}_p$ , and  $n$  bounded by some fixed  $N \in \mathbb{N}$ , so  $F$  satisfies the conditions of Theorem 3.1 when  $p > N$ .

Let  $C(r)$  be the collection of all permutations  $\sigma \in S_n$  with exactly  $r$  fixed points. If  $r = n$  then  $C(r)$  contains only the identity permutation and then  $\frac{\#C(r)}{\#S_n} = 1/n! = 1/r!$ . Otherwise, every  $\sigma \in C(r)$  can be written as  $\sigma = c_1 c_2 \cdots c_r \sigma_d$ , where each  $c_i$  is a length-one cycle and  $\sigma_d$  permutes the remaining elements and has no fixed points. Permutations that have no fixed points are called *derangements*, and the proportion of permutations that are derangements is extremely well-approximated by  $e^{-1}$  [11]. Specifically, the number of derangements of  $n$  elements is given by  $d_n = \lfloor e^{-1} n! \rfloor$ , where  $\lfloor \cdot \rfloor$  denotes the “nearest integer” function.

Therefore, to count the the number of  $\sigma \in C(r)$ , we simply count the ways to choose  $c_1, c_2, \dots, c_r$  and multiply by the number of derangements of the remaining  $n - r$  elements, so we have

$$\frac{\#C(r)}{\#S_n} = \frac{\binom{n}{r} d_{n-r}}{n!} = \frac{\frac{n!}{r!(n-r)!} d_{n-r}}{n!} = \frac{[e^{-1}(n-r)!]}{r!(n-r)!}.$$

Note that

$$\frac{[e^{-1}(n-r)!]}{r!(n-r)!} \leq \frac{e^{-1}(n-r)! + 0.5}{r!(n-r)!} \leq \frac{e^{-1} + 0.5}{r!} < \frac{1}{r!},$$

so in fact we have  $\frac{\#C(r)}{\#S_n} \leq 1/r!$  always.

Let  $\mathcal{A}(r)$  denote the number of  $(a, b) \in \mathbb{F}_p^2$  such that  $F(a, b, x) = x^n + ax^s + b \in \mathbb{F}_p[x]$  has exactly  $r$  linear factors. Since  $C(r)$  is the union of some number of conjugacy classes which is bounded in terms of  $N$ , we have

$$\left| \frac{\#\mathcal{A}(r)}{p^2} - \frac{\#C(r)}{\#S_n} \right| \leq \sum_{C_\lambda \subseteq C(r)} \left| \frac{\#\mathcal{A}_\lambda}{p^2} - \frac{\#C_\lambda}{\#S_n} \right| = O_N \left( \frac{1}{p^{1/2}} \right),$$

as  $p \rightarrow \infty$ , where the  $O$ -constant depends only on  $N$ . Now define

$$\mathcal{A}^*(r) = \{(a, b) \in (\mathbb{F}_p^*)^2 : x^n + ax^s + b \text{ has exactly } r \text{ distinct linear factors}\}.$$

$\mathcal{A}^*(r)$  differs negligibly from  $\mathcal{A}(r)$  since there are less than  $2p$  elements in  $\mathbb{F}_p^2 \setminus (\mathbb{F}_p^*)^2$ , and by [2, Proof of Proposition 3.1], the number of  $(a, b) \in \mathbb{F}_p^2$  such that  $x^n + ax^s + b$  has a root of multiplicity is bounded asymptotically by  $O_N(p)$ , so

$$\left| \frac{\#\mathcal{A}^*(r)}{p^2} - \frac{\#\mathcal{A}(r)}{p^2} \right| = O_N \left( \frac{1}{p} \right).$$

Finally, note that

$$\left| \frac{\#\mathcal{A}^*(r)}{(p-1)^2} - \frac{\#\mathcal{A}^*(r)}{p^2} \right| \leq 1 - \frac{(p-1)^2}{p^2} < \frac{2}{p}.$$

Therefore we have

$$\left| \frac{\#\mathcal{A}^*(r)}{\#(\mathbb{F}_p^*)^2} - \frac{\#C(r)}{\#S_n} \right| = O_N \left( \frac{1}{p^{1/2}} \right),$$

which proves the first claim, concerning trinomials with  $\gcd(n, s) = 1$ .

Recall the definitions

$$M_p = \{f \in \mathbb{F}_p[x] : \deg f < p\}$$

$$T_{p,N} = \{x^n + ax^s + b : (a, b) \in (\mathbb{F}_p^*)^2, 0 < s < n \leq N, \text{ and } \gcd(n, s, p-1) = 1\},$$

and recall that  $\mu(p, r)$  denotes the proportion of  $f \in M_p$  with  $R(f) = r$ , and that  $t_N(p, r)$  denotes the proportion of  $f \in T_{p,N}$  with  $R(f) = r$ . It is clear that  $t_N(p, r)$  is equal to the average value across all fractions

$$\frac{\#\mathcal{A}^*(r)}{\#(\mathbb{F}_p^*)^2}$$

which are associated to a trinomial  $x^n + Ax^s + B$  with  $0 < s < n \leq N$  and  $\gcd(n, s, p-1) = 1$ . It remains to study trinomials with  $\gcd(n, s, p-1) = 1$  but  $\gcd(n, s) > 1$ .

Suppose  $k = \gcd(n, s) > 1$ , and write  $n = kn'$  and  $s = ks'$  so that  $\gcd(n', s') = 1$ . If  $\gcd(n, s, p-1) = 1$ , then we must have  $\gcd(k, p-1) = 1$ , so the map  $x \rightarrow x^k$  permutes  $\mathbb{F}_p$ . Since  $x^n = (x^k)^{n'}$  and  $x^s = (x^k)^{s'}$ , it follows that the trinomials  $x^n + ax^s + b$  and  $x^{n'} + ax^{s'} + b$  have the same number of distinct roots in  $\mathbb{F}_p$ . Thus,  $t_N(p, r)$  is equal to the average of a collection of fractions which all satisfy

$$\frac{\#\mathcal{A}^*(r)}{\#(\mathbb{F}_p^*)^2} \leq \frac{1}{r!} + \frac{C_N}{p^{1/2}},$$

where  $C_N \in \mathbb{R}$  is a constant which depends only on  $N$ . It follows immediately that

$$\limsup_{p \rightarrow \infty} t_N(p, r) \leq 1/r!$$

for each  $r \leq N$ , and so

$$\limsup_{p \rightarrow \infty} \left( \max_{r \leq N} t_N(p, r) r! \right) \leq 1.$$

In [12], Leont'ev studies the generating function  $\phi(x) = \sum_{r=0}^{\infty} \mu(p, r) x^r$ , and shows that  $\phi(x)$  converges to  $e^{x-1}$  for  $x \in (0, 1]$ . Using the continuity theorem for generating functions [13, Section 1.1.6], he then concludes that  $\mu(p, r) \rightarrow e^{-1}/r!$  as  $p \rightarrow \infty$  for all  $r \in \mathbb{N}$ . Since we are only interested in the finitely many  $r \in \{0, 1, \dots, N\}$ , we can also be assured that

$$\lim_{p \rightarrow \infty} \left( \min_{r \leq N} \mu(p, r) r! \right) = e^{-1}.$$

Therefore, we have

$$\begin{aligned} \limsup_{p \rightarrow \infty} \left( \max_{r \leq N} \frac{t_N(p, r)}{\mu(p, r)} \right) &= \limsup_{p \rightarrow \infty} \left( \max_{r \leq N} \frac{t_N(p, r)}{\mu(p, r)} \frac{r!}{r!} \right) \\ &\leq \limsup_{p \rightarrow \infty} \left( \frac{\max_{r \leq N} t_N(p, r) r!}{\min_{r \leq N} \mu(p, r) r!} \right) \\ &= \frac{\limsup_{p \rightarrow \infty} (\max_{r \leq N} t_N(p, r) r!)}{\lim_{p \rightarrow \infty} (\min_{r \leq N} \mu(p, r) r!)} \\ &\leq \frac{1}{e^{-1}} \\ &= e. \end{aligned}$$

□

#### 4. POISSON HEURISTIC AND COMPUTATIONAL DATA FOR $\mathbb{F}_p$

First, we attempt to establish some basic plausibility for the Poisson Heuristic. As before, let  $t(p, r)$  denote the proportion of trinomials over  $\mathbb{F}_p$  with  $\delta = 1$  that have  $r$  distinct roots. The following table gives the statistical distance between  $t$  and a Poisson distribution with mean 1 for a few fields of various sizes.

$\mathbb{F}_p$	$\sum_{r=0}^{\infty}  t(p, r) - e^{-1}/r! $
$\mathbb{F}_{101}$	0.0367266
$\mathbb{F}_{1009}$	0.0112061
$\mathbb{F}_{10007}$	0.0007107
$\mathbb{F}_{100003}$	0.0000834

TABLE 1. Deviation of  $t(p, r)$  from a Poisson distribution.



Recall that  $T_p$  denotes the set of trinomials over  $\mathbb{F}_p$  with  $\delta = 1$  and degree less than  $p - 1$ . We have computed  $R_p$ , the maximum number of roots attained by any  $f \in T_p$ , for primes up to  $p = 139571$ . In this section, we show that the values of  $R_p$  that we would expect by Heuristic 1.4 are quite close to what we actually observe. That is, we consider the expected values of

$$R_p = \max\{R(f) : f \in T_p\}$$

under the model that the values of  $R(f)$  are given by random variables with distribution function  $\rho(r) = e^{-1}/r!$ , and we compare these expected values with real values of  $R_p$ .

More generally, let  $M_N$  be the maximum of  $N$  independent variables all with distribution  $\rho(r) = e^{-1}/r!$ . It is known that  $M_N$  becomes very predictable when  $N$  is large. Specifically, it is shown in [1] that there exists an integer sequence  $\widehat{M}_N$  such that, as  $N \rightarrow \infty$ ,

$$\text{Prob}(|\widehat{M}_N - M_N| \leq 1) \rightarrow 1.$$

In [10], a nice asymptotic formula is given for  $\widehat{M}_N$ :

$$\widehat{M}_N \sim \frac{\log N}{\log \log N}.$$

As an initial estimate, there are slightly less than  $p^4$  trinomials  $x^n + ax^s + b \in T_p$ : there are  $(p - 1)^2$  pairs  $(a, b)$  and almost  $(p - 1)^2$  pairs  $(n, s)$ . So, assuming Heuristic 1.4, a reasonable conservative prediction would be

$$R_p \approx \frac{4 \log p}{\log \log p}.$$

However, to make an accurate prediction for  $R_p$  we need to be more precise in two ways. Firstly, there are actually much fewer independent values of  $R(f)$  than  $p^4$ . For any  $f \in \mathbb{F}_p[x]$ , we have that

$$R(f(x)) = R(f(\gamma x^e)),$$

as long as  $\gcd(e, p - 1) = 1$  and  $\gamma \in \mathbb{F}_p^*$ , because the maps  $x \rightarrow \gamma x$  and  $x \rightarrow x^e$  are both bijections on  $\mathbb{F}_p$ . As a result, knowing the number of roots of one trinomial immediately determines the number of roots of a significant chunk of trinomials. Therefore, we would like to find an appropriate, effective value for  $N$  that better models the number of independent random values. To do this, we count exactly the number of trinomials with  $\delta = 1$  and then quotient out by the size of these equivalent chunks.

The exact number of pairs  $(n, s)$  that are relatively prime with  $p - 1$  is given by the *Jordan totient function*,  $J_2(p - 1)$  [8, p. 147]. We must subtract  $\varphi(p - 1)$  to avoid counting pairs with  $n = s$ , and we divide by 2 to avoid counting both  $(n, s)$  and  $(s, n)$ . There are  $(p - 1)^2$  choices for the two coefficients, so overall we have

$$\#T_p = (1/2) (p - 1)^2 (J_2(p - 1) - \varphi(p - 1)).$$

As discussed in Section 2,  $\gcd(n, s, p - 1) = 1$  implies that every pair  $(\gamma^n, \gamma^s)$  is unique, so we divide by  $(p - 1)$  to account for trinomials of the form  $f(\gamma x)$ . To account for the transformation  $x \rightarrow x^e$ , we divide by the number of  $e$  with  $\gcd(e, p - 1) = 1$ , which is given by  $\varphi(p - 1)$ . So, we take our effective number of independent Poisson variables to be

$$N(p) = \left( \frac{p - 1}{2} \right) \left( \frac{J_2(p - 1)}{\varphi(p - 1)} - 1 \right).$$

This number is approximately equal to  $p^2$ ; for primes in the range  $11 \leq p \leq 139571$ , we have

$$\frac{1}{2} < \frac{N(p)}{p^2} < 2.$$

Secondly, it is beneficial to consider the less elegant but more precise asymptotic formula for  $\widehat{M}_N$  given in [4]. Below,  $W$  is the *Lambert W function*.

$$\widehat{M}_N \sim E_N := \frac{\log N}{W(\log(N)/e)} - \frac{1 + \log 2\pi}{2 \log \left( \frac{\log N}{W(\log(N)/e)} \right)} - 1.5.$$

In summary, by Heuristic 1.4 we expect that  $R_p \approx E_{N(p)}$  when  $p$  is sufficiently large. The following plot displays the ratios  $R_p/E_{N(p)}$  for all primes  $p \leq 139571$ .

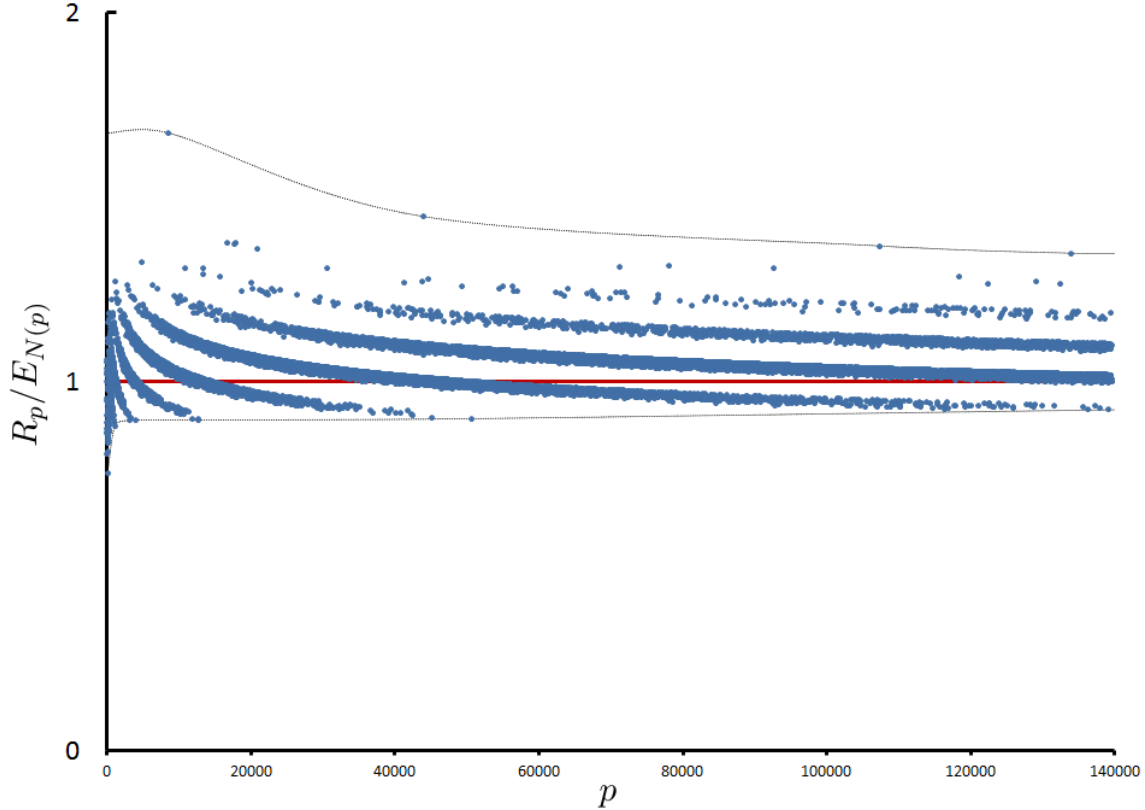


FIGURE 1. The ratios  $R_p/E_{N(p)}$  for all primes  $p \leq 139571$ .

The visibly distinct bands correspond to primes that share the same value for  $R_p$ . The apparent upper and lower bounding monotonic subsequences are traced by dotted curves. The average over all ratios is 1.0429 and the standard deviation is 0.05587. For all  $p \leq 139571$ , we have  $R_p \leq 2 \log p$ . The largest recorded value of  $R_p$  is  $R_p = 16$ , which is witnessed at  $p = 8581, 43943, 107351$ , and  $133877$ ; the associated ratios  $16/E_{N(p)}$  lie visibly on the upper dotted line.

The values of  $R_p = \max\{R(f) : f \in T_p\}$  were computed in a straightforward way (i.e. by enumerating trinomials and counting their roots) by parallel C++ code which ran on Texas A&M's Ada supercomputing cluster for 5000 CPU hours. The program takes advantage of the fact that  $R(f(x)) = R(f(\gamma x^e))$  when  $\gcd(e, p-1) = 1$  and  $\gamma \in \mathbb{F}_p^*$  to reduce the enumeration space. The values  $E_{N(p)}$  were computed separately by a small Matlab program, which in particular makes use of Matlab's built-in `lambertw` function.

#### ACKNOWLEDGMENTS

We would like to thank the Texas A&M Supercomputing Facility for providing us with computational resources, and our advisor, J. Maurice Rojas, for his indispensable guidance.

## REFERENCES

- [1] Anderson, C.W., 1970. Extreme value theory for a class of discrete distributions with applications to some stochastic processes. *Journal of Applied Probability*, pp. 99-113.
- [2] Bank, E., Bary-Soroker, L. and Rosenzweig, L., 2015. Prime polynomials in short intervals and in arithmetic progressions. *Duke Mathematical Journal*, 164(2), pp.277-295.
- [3] Bi, J., Cheng, Q. and Rojas, J.M., 2013, June. Sub-linear root detection, and new hardness results, for sparse polynomials over finite fields. *Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation* (pp. 61-68). ACM.
- [4] Briggs, K.M., Song, L. and Prellberg, T., 2009. A note on the distribution of the maximum of a set of Poisson random variables. *arXiv preprint arXiv:0903.4373*.
- [5] Canetti, R., Friedlander, J., Konyagin, S., Larsen, M., Lieman, D. and Shparlinski, I., 2000. On the statistical properties of Diffie-Hellman distributions. *Israel Journal of Mathematics*, 120, pp.23-46.
- [6] Cheng, Q., Gao, S., Rojas, J.M. and Wan, D., 2014. Sparse univariate polynomials with many roots over finite fields. *arXiv preprint arXiv:1411.6346*.
- [7] Cohen, S., 1980. The Galois group of a polynomial with two indeterminate coefficients. *Pacific Journal of Mathematics*, 90(1), pp.63-76.
- [8] Dickson, L.E., 1919. *History of the theory of numbers, Vol. I*, Carnegie Institution, Washington DC.
- [9] Kelley, Z., 2016. Roots of sparse polynomials over a finite field. *arXiv preprint arXiv:1602.00208*.
- [10] Kimber, A.C., 1983. A note on Poisson maxima. *Probability Theory and Related Fields*, 63(4), pp.551-552.
- [11] Hassani, M., 2003. Derangements and applications. *Journal of Integer Sequences*, 6(2), p.3.
- [12] Leontev, V.K., 2006. Roots of random polynomials over a finite field. *Mathematical Notes*, 80(1), pp.300-304.
- [13] Sachkov, V.N., 1997. *Probabilistic methods in combinatorial analysis*. Cambridge University Press, Cambridge.